Before the
Federal Communications Commission
Washington, D.C. 20554

Communications Assistance for Law Enforcement Act and Broadband Access and Services	ET Docket No. 04-295 RM-10865

Reply Comments of the Satellite Industry Association

David Cavossa
Executive Director
Satellite Industry Association
1730 M Street, N.W., Suite 600
Washington, DC 20036

(202) 349-3651

Table of Contents

I. Introduction and Summary 1

II. The Commission Should Clarify the Scope of Broadband Internet Access and Managed VOIP Providers' CALEA Obligations 3

A. The Commission Should Clarify that Most FSS Services Are Not Subject to CALEA 4

B. The Commission Should Clarify Which VOIP Services, if Any, It Makes Subject to CALEA in this Proceeding 5

C. The Record Supports SIA's Position that a Broadband Internet Access Provider Should Not Be Responsible for Extracting Call-Identifying Information Relating to Services It Does Not Provide 7

D. The Commission Should Not Mandate Needless Additional Complexity Beyond that Already Required by the CALEA Statute 9

III. The Commission Should Provide Adequate Time for CALEA Solutions to be Developed and Implemented 13

A. Standard-Setting Organizations and Industry Associations Have a Crucial Role to Play in the CALEA Implementation Process 13

B. Providers of Broadband Internet Access and Managed VOIP Services Should Not Be Required to Implement CALEA Prematurely 14

IV. Conclusion 17

Before the
Federal Communications Commission
Washington, D.C. 20554

Communications Assistance for Law Enforcement Act and Broadband Access and Services	ET Docket No. 04-295 RM-10865

Reply Comments of the Satellite Industry Association

The Satellite Industry Association ("SIA") offers the following reply comments on the Commission's above-captioned Notice of Proposed Rulemaking ("Notice") on the application of the Communications Assistance for Law Enforcement Act ("CALEA") to broadband access and services.[1] SIA previously filed comments in this proceeding on November 8, 2004.

I. Introduction and Summary

The satellite industry today offers a vibrant array of facilities and services to its customers, including equipment manufacturing, facilities leasing, private network and private carrier services, and some common carriage. These services are offered by fixed-satellite service ("FSS") and mobile-satellite service ("MSS") providers.[2]

In its initial comments in this proceeding, SIA urged the Commission to recognize that:

---

[1] *Communications Assistance for Law Enforcement Act and Broadband Access and Services,* ET Docket No. 04-295, Notice of Proposed Rulemaking, FCC 04-187, 19 FCC Rcd 15676 (2004). Comments were due November 8, 2004. The Office of Engineering and Technology subsequently extended the reply comment deadline to December 21, 2004. *Communications Assistance for Law Enforcement Act and Broadband Access and Services*, ET Docket No. 04-295, Order Granting Extension of Time, DA 04-3682 (O.E.T. rel. Nov. 24, 2004).

[2] The third main category of satellites services, broadcasting-satellite service ("BSS"), is not subject to CALEA and is not at issue in this proceeding.

- Most FSS services, equipment, and facilities, including bare space segment and those non-public and intracorporate networks supported by FSS capacity, are not subject to CALEA;

- There is no need for system-by-system agreements to implement CALEA for satellite-delivered broadband Internet access and managed VOIP services because CALEA capabilities should be incorporated into the routers used by satellite-based and terrestrial providers;

- Compliance with an order authorizing law enforcement to intercept the full content of a user's communications can be achieved by delivering to law enforcement the packet stream, as captured by network analyzers or "sniffers";

- With respect to call-identifying information, the broadband Internet access provider should not be required to provide information other than the information contained in the transport layer headers, which is the only information reasonably available to the broadband Internet access provider;

- It should be the responsibility of the managed VOIP application provider to collect and provide to law enforcement any additional call-identifying information associated with a managed VOIP call other than that which the transportation provider of the "call" can provide;

- The statutory terms "industry associations" and "standards-setting organizations" should be interpreted as broadly as possible to ensure that all interested parties are able to participate in the development of CALEA safe harbor standards; and

- The Commission should afford broadband Internet access and managed VOIP application providers a reasonable time period to adjust to the Commission's reinterpretation of CALEA, measured as one year from the latest of the dates on which (1) one or more industry associations or standard-setting organizations establish safe harbor standards that are generally agreed to meet the CALEA capability requirements; (2) the Attorney General issues a final notice of capacity applicable to entities providing any services the Commission finds subject to CALEA in this proceeding; and (3) the Commission establishes system security and integrity rules applicable to such entities.

The record developed during the initial comment phase of this proceeding contains broad support for all of these points. SIA urges the Commission to follow these principles in developing any rules it may issue in this proceeding.

In these reply comments, SIA responds to the additional record information in this proceeding and makes the following specific points:

- The Commission should clarify the scope of broadband Internet access and managed VOIP providers' CALEA obligations, including clarifying that many FSS services are not subject to CALEA;
- The Commission should clearly identify which VOIP services it intends to make subject to CALEA, as the definition of "managed VOIP" in the Notice is unworkable;
- A providers of broadband Internet access should not be responsible for providing call identifying information relating to services it does not provide to the end user;
- The Commission should reject proposals in the record to needlessly complicate CALEA compliance by mandating system-by-system compliance agreements by satellite-based providers of broadband Internet access or managed VOIP services, requiring multinational providers to use "transnational trusted third parties" to achieve compliance, expanding CALEA to cover stored communications, or precluding the use of packet "sniffing" technology;
- The Commission should provide adequate time for safe harbor compliance standards to be incorporated into network equipment and deployed by service providers.

II. The Commission Should Clarify the Scope of Broadband Internet Access and Managed VOIP Providers' CALEA Obligations

In their initial comments in this proceeding, SIA, the United States Internet Service Providers' Association ("USISPA"), and other commenters raised significant issues concerning the intended scope of the Commission's Notice in this proceeding. Any lack of perfect clarity regarding the precise services that the Commission intends to make subject to CALEA could have the unintended consequence of hindering industry efforts to comply with CALEA. SIA believes that two areas in particular generate the greatest concern, as follows:

A. The Commission Should Clarify that Most FSS Services Are Not Subject to CALEA

In its initial comments, SIA explained that there are many services that FSS satellite providers offer to their customers that do not fall within the boundaries of the statute. SIA specifically supported the Commission's recognition that entities that sell or lease facilities – including bare space segment capacity – on a non-common carrier basis, are not subject to the requirements or CALEA.[3] The record developed in the initial comment round contains no significant dispute on this point. In this respect, SIA strongly supports the USISPA's argument that the Commission should clarify that CALEA obligations should be limited to "telecommunications transmission services that are a component of broadband [Internet] access services."[4]

If the Commission determines that broadband Internet access providers should be subject to CALEA, it should limit the scope of this determination as defined by USISPA. As explained by SIA in its initial comments, if the Commission relies upon the "substantial replacement" provision of CALEA to subject broadband Internet access to that statute's requirements, this language can only apply to "last mile"-type transmission services provided to end users. Neither the "substantial replacement" provision nor any other provision of CALEA applies to long-haul, Internet backbone and similar services that FSS providers offer to Internet service providers or to connect other carriers. Indeed, these services are specifically exempted. *First*, CALEA specifically exempts carriers that merely interconnect other carriers from its ambit.[5] As the USISPA explains, Internet backbone services are the IP equivalent of circuit-

---

[3] Notice at para. 37 and n.80; SIA Comments at 3.

[4] USISPA Comments at 11.

[5] 47 U.S.C. § 1002(b)(2)(B).

switched interexchange services, which interconnect local exchange carriers. The Commission has long held that carriers are not subject to CALEA to the extent that they provide such interexchange services. *Second*, even if covered, the statute expressly requires surveillance to be conducted "in a manner that protects the privacy and security of communications and call-identifying information not authorized to be intercepted."[6] In enacting this requirement, Congress explicitly recognized that, "courts should scrutinize very carefully requests to intercept trunk lines and insist that agencies specify how they will comply" with the requirement to safeguard other communications that are not the subject of the surveillance request.[7] Surveillance of Internet backbone trunks could not be accomplished in a manner consistent with these limitations the statute imposes to protect the privacy of communications that are not the subject of an intercept order. *Third*, as a practical matter, because of the diverse routing of individual IP packets, surveillance conducted on an Internet backbone trunk would not produce a complete record of the subject's communications, as some of the packets destined to or from the subject would almost certainly take other routes to their destination.

B. The Commission Should Clarify Which VOIP Services, if Any, It Makes Subject to CALEA in this Proceeding

The Commission's Notice in this proceeding tentatively concluded that providers of VOIP services that allow a user to communicate with any telephone subscriber, including those reachable only via the public switched telephone network ("PSTN"), should be subject to CALEA, while those that permit a user to communicate only within a defined user group should not. SIA understands the Commission's goal and supports the Commission's proposal in the Notice to find that VOIP communications wholly within the Internet or a private IP network

---

6 47 U.S.C. § 1002(a)(4)(A).

7 House Report No. 103-827, 1994 U.S.C.C.A.N. 3489, 3504.

(1) are excluded from CALEA by the statute's "private networks" exemption,[8] and (2) do not replace a substantial portion of the customer's local exchange service.[9]

Rather than attempting to segregate VOIP services into "managed" and "non-managed" categories, however, SIA urges the Commission to create a bright line test based on this distinction. In adopting rules in this proceeding, therefore, the Commission should state clearly that it intends the amended CALEA rules and requirements to apply only to audio-only VOIP communications that originate from or terminate with a user of the public switched telephone network ("PSTN"), and that the new rules for CALEA do not cover any VOIP communications that both originate and terminate on IP-based networks.[10] By clarifying this point, the Commission will circumscribe the range of technical issues that industry associations and standard-setting organization must resolve in developing safe harbor compliance standards for VOIP services.

This point is important to SIA members because, in their capacity as providers of broadband Internet access service, SIA members likely will need to be involved in the interception of VOIP call content information. A customer that initiates a VOIP call initially transmits Session Initiation Protocol ("SIP") or H.323 signaling information to the VOIP provider's server, whether the service permits communication with users of the PSTN or not. The managed VOIP provider responds with information necessary for the content of the VOIP call to be routed between the initiating customer and the call recipient(s). At that time, the packets containing the content of the call are routed directly to the location of the call recipient(s), and not to the VOIP service provider, whether the recipient of the call is located on

---

8 47 U.S.C. § 1002(b)(2)(B).

9 Notice at para. 58.

10 SIA intends its use of the term "managed VOIP services" (and similar phrases) in this sense.

an IP network or the circuit-switched PSTN. If the recipient is located on the PSTN, the packets will be routed to one or more gateways between the circuit- and packet-switched networks. If the recipient of the call is located on an IP network, the packets will, in the ordinary case, be routed directly to the recipient's network address. Finally, at the time the call is completed, SIP or H.323 signaling information communicates that fact to the VOIP provider.

Thus, there is no practical way to distinguish between a "peer-to-peer" call (*i.e.*, IP-to-IP) completed using the services of a VOIP provider that allows interconnection with the PSTN and one that does not, and no policy reason to subject one such call to the strictures of CALEA, while exempting the other. In either case, the VOIP provider should be able to provide the Commission with call-identifying information such as the time and duration of the call and the called party number, while the content of the call likely will need to be intercepted at its source by the broadband Internet access provider. Only calls that actually connect a VOIP user to users of the PSTN, however, truly provide a "replacement for a substantial portion of the [VOIP user's] local telephone exchange service." As such, only VOIP calls that actually connect to the PSTN should be subject to CALEA.

C. The Record Supports SIA's Position that a Broadband Internet Access Provider Should Not Be Responsible for Extracting Call-Identifying Information Relating to Services It Does Not Provide

As SIA explained in its initial comments,[11] the best and most efficient way for terrestrial and satellite-based broadband Internet access providers and managed VOIP providers alike to implement CALEA is for equipment manufacturers to implement a safe harbor CALEA compliance standard, when available, in standard routers. To facilitate the development of such a standard, the Commission should clarify that, with respect to a broadband Internet access

[11] SIA Comments at 12-13.

provider, the only call-identifying information that is "reasonably available to the carrier," 47 U.S.C. § 1002(a)(2), is that information available in the transport layer headers of the packets a customer sends or receives.

SIA agrees with the Department of Justice ("DOJ"), the USISPA and, indeed, the Commission itself, that a broadband Internet access provider should NOT be responsible for extracting any additional call identification information that may be available in the user's packet stream, particularly if it pertains to services, such as VOIP, that the broadband Internet access provider does not provide to the end user.[12] Such information cannot be obtained by a broadband Internet access provider without breaking open the information packets and examining the contents. It is likely to be outright impossible for the broadband Internet access provider to gain access such content information, as it may be encrypted, or encoded using proprietary formats unique to the individual application that generated the packets. Even if it were possible, the broadband Internet access provider does not routinely examine or use such information for its own purposes, making it extremely costly and burdensome for the broadband Internet access provider to gather such information.

Rather, as the USISPA argues, call-identifying information is only "reasonably available" if the provider uses the information in serving its customer.[13] Under this formulation, the subject's managed VOIP provider would be responsible for providing any additional call-identifying information, which should be available to the managed VOIP provider from its SIP

---

[12] Notice at para. 56 ("We understand that basic capabilities essential to Law Enforcement's surveillance efforts, such as access to call management information . . . and call setup information . . . may not be reasonably available to the broadband access provider."); DOJ Comments at 7-8; USISPA Comments at 19.

[13] USISPA Comments at 19.

or H.323 protocol information it uses to initiate, manage, and terminate communication sessions between VOIP network endpoints.

D. The Commission Should Not Mandate Needless Additional Complexity Beyond that Already Required by the CALEA Statute

The Commission should reject arguments leveled in initial comments that would needlessly complicate CALEA compliance and, in some cases, go well beyond the boundaries of the statute. Specifically, among other burdensome, unnecessary, and needlessly complicated proposals these commenters make, SIA urges that the Commission NOT (1) mandate the use of system-by-system agreements for satellite-based providers of broadband Internet access or managed VOIP services;[14] (2) mandate use of "transnational trusted third parties" for CALEA compliance by multinational communications providers;[15] (3) subject stored data to the inapposite requirements of CALEA;[16] or (4) preclude the use of network analyzers, or "sniffers" in CALEA compliance.[17] Arguments that the Commission adopt such requirements are nothing more than attempts to increase the cost and complexity of CALEA compliance by commenters developing businesses that would provide the CALEA functionality they propose to be mandatory.

First, with respect to system-by-system agreements, as SIA explained in its comments, satellite-based providers of broadband Internet access or managed VOIP services use the same routers and transmission protocols in providing service that terrestrial providers use and therefore, in the vast majority of cases, they will be able to use the same CALEA compliance standards as these terrestrial providers. Quite simply, there is no need for satellite-specific

---

[14] Verisign Comments at 27.

[15] Verisign Comments at 27-29.

[16] Verisign Comments at 31-32.

[17] Fiducianet Comments at 26.

standards or individualized agreements to achieve CALEA compliance for satellite-delivered broadband Internet access or managed VOIP services as they are provided today. While Verisign argues that such an ad hoc, system-by-system approach would "represent[] a pragmatic and appropriate approach" and be "consonant with decisions taken internationally by law enforcement and standards bodies,"[18] it offers no convincing support for this position. While Verisign cites the minutes from the June 2004 meeting of the ETSI Technical Committee on Satellite Earth Stations and Systems ("TC SES"), Verisign at 27, n.50, that document in fact records the decision of the TC SES *not* to take any action with respect to lawful interception issues.[19] Furthermore, even the ETSI Technical Committee on Lawful Interception ("TC LI"), which has primary responsibility for these issues, has no authority to control "decisions taken internationally by law enforcement and standards bodies." Rather, TC LI can only make standards *recommendations* for consideration by regional governments. These governments, in turn, may adopt rules consistent with the recommended standards, expand on them, or modify them as they see fit.

Furthermore, to the extent that Verisign's position is based on the transnational capability of satellite-based networks, this fact does little to distinguish satellite-based providers from any number of terrestrial providers with global fiber networks.

---

[18] Verisign Comments at 27.

[19] By way of background, in January 2004, TC SES decided to form an ad hoc group charged with considering issues related to lawful interception on satellite networks. At the next meeting, in June, 2004, the ad hoc group reported its conclusion that the ETSI Technical Committee on Lawful Interception ("TC LI") was already studying these issues, and that there was no need for additional work by TC SES at that time. The TC SES determined to keep the item on its agenda, but has done no further work on these issues.

Second, with respect to the use of "transnational trusted third parties,"[20], SIA acknowledges the burden placed on multinational service providers by the multiplicity of individual national surveillance standards existing around the world. Indeed, the Convention on Cybercrime, which Verisign cites as evidence of the need for transnational trusted third parties, represents a significant step toward creating more harmony and uniformity among these standards. For some multinational providers of broadband Internet access and managed VOIP services, a transnational trusted third party may represent a cost-effective solution that simplifies the provider's efforts to discharge its compliance obligation, and SIA agrees that such an option should be available. The Commission, however, should not *require* any multinational provider of broadband Internet access and managed VOIP services to employ the services of such a transnational trusted third party, if it can instead achieve compliance of its own accord.

Third, contrary to the argument of Verisign, the Commission should recognize that CALEA does not apply to stored communications. Rather, the purpose of CALEA is to "make clear a telecommunications carrier's duty to cooperate in the *interception* of communications for law enforcement purposes."[21] It does not, of its own terms, create any basis or procedure for law enforcement to seek judicial authorization to conduct surveillance activities. It simply mandates that, once that authorization has been granted, certain surveillance capabilities must be available in the network.[22] By its terms, it speaks of surveillance in real time – it mandates that law enforcement must be able to "intercept . . . wire and electronic communications," 47 U.S.C. § 1002(a)(1) and "access call identifying information . . . *before*,

---

[20] Verisign Comments at 27-29.

[21] Preamble to Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (emphasis added).

[22] 47 U.S.C. § 1002(a).

during, or immediately after" the communication occurs, 47 U.S.C. § 1002(a)(2)(A). The statute does not in any way contemplate storage of communications or access to any communications that might happen to be stored. Furthermore, Commission interpretation of CALEA to broaden CALEA into the realm of stored communications could substantially delay the development of compliance standards as industry associations and standard setting organizations would have to consider the additional issues such action would create. Even once these standards were developed, such a requirement would substantially increase the cost of implementing CALEA in provider networks because it would require deployment of substantial additional storage capacity that is generally not present today.[23]

Moreover, such an expansion of CALEA is fundamentally unnecessary to provide law enforcement with access to stored communications. Other statutes, including the Stored Communications Act, already explicitly provide for law enforcement access to such communications, stating, for example, that "a governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system . . . pursuant to a warrant . . . ."[24]

Fourth, the Commission should recognize the important role that network analyzers, or "packet sniffers" can play in achieving CALEA compliance. Fiducianet opposes the use of sniffers, arguing that situations will arise in which "the content flow will not be visible to sniffers in the network."[25] Once again, this argument is interposed merely to create needless

---

[23] *See* SIA Comments at 10.

[24] *See, e.g.*, 18 U.S.C. § 2703(a).

[25] Fiducianet Comments at 26; *see also* DOJ Comments at 19-20 (use of packet sniffing ignores critical privacy issues because the subject's packets cannot be isolated).

complexity around CALEA compliance. As SIA explained in its initial comments, sniffers have the capability to efficiently filter packets sent from or received by a particular subject, as identified by the source or destination IP address and port, and output the isolated packet stream in a standard format. Because the sniffer will only be effective in accomplishing this goal if the subject's packets pass though the router where the sniffing occurs, it is important for the broadband Internet access or managed VOIP provider to choose a location in close network proximity to the surveillance subject, at the first router to which the subject directly connects. While SIA agrees with Fiducianet that, if a provider chooses to place the sniffer incorrectly, it may not intercept the subject's full packet stream, this merely underscores the importance of the location choice, and does nothing to call into question the value of the sniffing technology.

III. The Commission Should Provide Adequate Time for CALEA Solutions to be Developed and Implemented

A. Standard-Setting Organizations and Industry Associations Have a Crucial Role to Play in the CALEA Implementation Process

SIA agrees with the DOJ that the Commission should not try to resolve all of the remaining open technical issues associated with the development of safe harbor CALEA compliance standards for broadband Internet access and managed VOIP services.[26] As SIA explained in its initial comments, the statute expresses a clear preference for private development of standards.[27] Rather than preempting the private standard-setting process, the Commission should clarify the scope of the services to which CALEA applies in this order, and allow industry associations and standard-setting bodies that are developing compliance standards to work within that clarified Commission framework.

---

[26] DOJ Comments at 39-42.

[27] 47 U.S.C. § 1006(a); SIA Comments at 14.

As a corollary, and to facilitate widespread efforts and the highest level of creativity on the development of safe harbor CALEA compliance standards, the Commission should adopt the broadest possible interpretation of the statutory terms "industry association" and "standard-setting organization."[28] SIA appreciates the goal of the three criteria proposed by the DOJ.[29] Nevertheless, SIA is concerned that these criteria are unnecessary and will be difficult to apply in practice, and add little to the integrity of the standard that an association might develop. For example, the DOJ makes no attempt to explain how to determine when an industry association or standard-setting organization is "generally recognized," or what would constitute an "adequate" record of its proceedings.[30] Further, the answers would appear ultimately irrelevant if the body in question produced a workable compliance standard, and the statute vests the Commission with authority to decide that ultimate question in any event.[31]

B. Providers of Broadband Internet Access and Managed VOIP Services Should Not Be Required to Implement CALEA Prematurely

As SIA explained in its initial comments, there is a tremendous amount of work to be done before broadband Internet access and managed VOIP providers can become fully compliant with CALEA.[32] As SIA explained, newly-covered entities would be obligated to

---

[28] TIA and ETSI should undoubtedly qualify as standard-setting organizations in any event, as they argued in their respective comments. TIA Comments at 10-13; ETSI Comments at 2-3.

[29] DOJ Comments at 54-56 (arguing that an "industry association" or "standard-setting organization" should (1) be generally recognized as representative of the telecommunications industry and having technical expertise to engage in the specialized process of developing a technical telecommunications standard; (2) expressly state in the standard it develops that it is intended to guide CALEA compliance for a specific scope of telecommunications carriers; and (3) maintain an adequate record of its proceedings, including technical capabilities considered, those rejected, and the reason for the rejection.).

[30] DOJ Comments at 55.

[31] 47 U.S.C. § 1006(b); *see* TIA Comments at 12-13.

[32] SIA Comments at 16-18.

comply with the capability requirements of Section 103, the capacity requirements of Section 104, and the system security and integrity requirements of Section 105.[33] As yet, neither the Commission, nor the Attorney General, nor industry associations nor standard-setting organizations have adopted rules or standards implementing any of these requirements.

Therefore, SIA strongly opposes the DOJ's proposal that the Commission impose a CALEA compliance obligation immediately upon the issuance of its order in this proceeding, whether the Commission also provides a separate 12-month deadline to deploy and make available CALEA-compliance intercept solutions.[34] Despite the DOJ's wishes, newly-covered providers of these services simply will not be able to achieve compliance by this date. Many factors upon which compliance depends are not currently within the control of the individual providers of these services. Moreover, one year is simply not enough time to develop implementing rules and standards for Sections 103, 104, and 105 of CALEA, let alone manufacture compliant equipment and deploy it throughout a network. As a result, the Commission will merely sow chaos and uncertainty if it attempts to set an unrealistic compliance deadline, and could inadvertently delay the achievement of CALEA compliance, as providers divert resources to seek exemptions, waivers, or extensions of time to comply with the Commission's rules.

SIA proposed a compliance deadline of one year from the latest of the dates on which (1) one or more industry associations or standard-setting organizations establish safe harbor safeguards that are generally agreed to meet the CALEA capability requirements of Section 103, or the date on which the Commission's order resolving any petitions filed pursuant to Section 107(b) takes effect; (2) the Attorney General issues a final notice of capacity

---

[33] *Id.*

[34] DOJ Comments at 56-58; *see also id.* at 65, 75-76.

applicable to entities providing any services the Commission finds are subject to CALEA in this proceeding; and (3) the Commission establishes system security and integrity rules applicable to such entities.[35]

SIA's proposal enjoys broad support in the record. NCTA, for example, correctly argues that capacity standards must be adopted before imposing CALEA obligations on providers of broadband Internet access and managed VOIP services.[36] Furthermore, USISPA proposes a compliance timeline that is roughly equivalent to the SIA proposal, where a three-year compliance deadline for call-identification information and a 15 month deadline for call content information would be established, *as measured from the date of adoption of a CALEA safe harbor standard*.[37]

---

[35] SIA comments at 17-18.

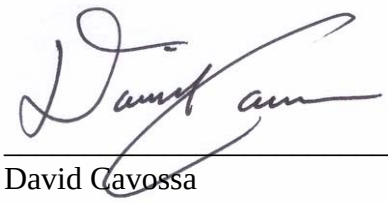
[36] NCTA Comments at 14-15.

[37] *See* USISPA Comments at 34-37.

IV. Conclusion

For the foregoing reasons, the Commission should adopt rules in this proceeding that (1) clarify that most FSS services are not subject to CALEA; (2) clearly identify which VOIP services it intends to make subject to CALEA; (3) clarify that providers of Broadband Internet access should not be responsible for providing call identifying information relating to services it does not provide to the end user, (4) reject proposals in the record to needlessly complicate CALEA compliance for the sole benefit of entities launching "trusted third party" CALEA outsourcing businesses, and (5) provide adequate time for safe harbor compliance standards to be incorporated into network equipment and deployed by service providers.

Respectfully submitted,



David Cavossa
Executive Director
Satellite Industry Association
1730 M Street, N.W., Suite 600
Washington, DC 20036
(202) 349-3651

December 21, 2004

DC\729969.1